Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1-9. (Canceled)

10. (Currently amended) A method for providing access management through use of a plurality of server machines associated with different locations, the method comprising:

(a)   authenticating a user with a first server machine of the plurality of server machines with respect to a prior access request;

(b)   subsequently receiving a current access request to access a secured item via a second server machine of the plurality of server machines; and

(c)   upon receiving the current access request to access the secured item via the second server machine, reconfiguring the first server machine to prevent further access by the user to secured items via the first server machine; and

(d)   upon receiving the current access request to access the secured item via the second server machine, reconfiguring the second server machine to permit access by the user to at least the secured item via the second server machine.

11. (Currently amended) A—The method as recited in claim 10, wherein the authenticating (a) authenticates both the user and a client machine being used by the user.

12. (Currently amended) A—The method as recited in claim 10, wherein the first

server machine and the second server machine are access points for the user to gain

access to secured items.

13. (Currently amended) A—The method as recited in claim 10, wherein when

the user is at a first location, the user interacts over a network with the first server

machine using a first client machine at the first location, and

wherein when the user is at a second location, the user interacts over a network

with the second server machine using a second client machine at the second location.

14. (Currently amended) A—The method as recited in claim 10, wherein the

method further comprises:

determining, prior to reconfiguring (c) or (d), whether the user is permitted to

gain access from a second location to secured items via the second server machine.

15. (Currently amended) A—The method as recited in claim 10, wherein

authenticating (a) of the user occurs while the user is at a first location, and wherein

receiving (a) of the access request to access the secured item from the user occurs while

the user is at a second location.

16. (Currently amended) A—The method as recited in claim 10, wherein the

method further comprises:

(e)   determining permitted locations from which the user is permitted to gain

access to secured items;

(f)   determining, prior to reconfiguring (c) or (d), whether the second location

is one of the permitted locations for the user; and

(g)   bypassing reconfiguring (c) or (d) when determining (f) determines that

the second location is not one of the permitted locations for the user.

17.   (Currently amended) A—The method as recited in claim 16, wherein when

the user is at the first location, the user interacts over a network with the first server

machine using a first client machine at the first location, and wherein when the user is at

the second location, the user interacts over a network with the second server machine

using a second client machine at the second location.

18.   (Currently amended) A computer readable medium including at least

computer program code for providing access management through use of a plurality of

server machines associated with different locations, the computer readable medium

comprising:

computer program code for authenticating a user with a first server machine of

the plurality of server machines with respect to a prior access request;

computer program code for subsequently receiving a current access request to

access a secured item via a second server machine of the plurality of server machines;

- 6 -

Hildebrand et al.
Appl. No. 10/076,181

computer program code for, upon receiving the current access request to access the secured item via the second server machine, reconfiguring the first server machine to prevent further access by the user to secured items via the first server machine; and

computer program code for, upon receiving the current access request to access the secured item via the second server machine, reconfiguring the second server machine to permit access by the user to at least the secured item via the second server machine.

19.   (Currently amended) A—The computer readable medium as recited in claim 18, wherein when the user is at a first location, the user interacts over a network with the first server machine using a first client machine at the first location, and

wherein when the user is at a second location, the user interacts over a network with the second server machine using a second client machine at the second location.

20.   (Currently amended) A—The computer readable medium as recited in claim 18, further comprising:

computer program code for determining, prior to the reconfiguring of either the first server machine or the second server machine, whether the user is permitted to gain access from a second location to secured items via the second server machine.

21.   (Currently amended) A system for providing access management through use of a plurality of server machines associated with different locations, comprising:

means for authenticating a user with a first server machine of the plurality of server machines with respect to a prior access request;

means for subsequently receiving a current access request to access a secured item via a second server machine of the plurality of server machines;

means for, upon receiving the current access request to access the secured item via the second server machine, reconfiguring the first server machine to prevent further access by the user to. secured items via the first server machine; and

means for, upon receiving the current access request to access the secured item via the second server machine, reconfiguring the second server machine to permit access by the user to at least the secured item via the second server machine.

22. (New) The computer readable medium as recited in claim 18, wherein said computer program code for authenticating a user with a first server machine comprises:

computer program code for authenticating both the user and a client machine being used by the user.

23. (New) The computer readable medium as recited in claim 18, further comprising:

computer program code for determining, prior to reconfiguring the first and second server machines, whether the user is permitted to gain access from a second location to secured items via the second server machine.

24. (New) The computer readable medium as recited in claim 18, further comprising:

computer program code for determining permitted locations from which the user is permitted to gain access to secured items;

computer program code for determining, prior to reconfiguring the first and second server machines, whether the second location is one of the permitted locations for the user; and

computer program code for bypassing reconfiguring the first and second server machines, if it is determined that the second location is not one of the permitted locations for the user.

25. (New) The system of claim 21, wherein said means for authenticating comprises means for authenticating both the user and a client machine being used by the user.

26. (New) The system of claim 21, wherein the first server machine and the second server machine are access points for the user to gain access to secured items.

27. (New) The system of claim 21, further comprising:

means for determining, prior to reconfiguring the first and second server machines, whether the user is permitted to gain access from a second location to secured items via the second server machine.

28. (New) The system of claim 21, further comprising:

means for determining permitted locations from which the user is permitted to gain access to secured items;

means for determining, prior to reconfiguring the first and second server machines, whether the second location is one of the permitted locations for the user; and

means for bypassing reconfiguring the first and second server machines if it is determined that the second location is not one of the permitted locations for the user.